Journal of the Faculty of Engineering and Architecture of Gazi University 39:1 (2024) 509-519

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University
Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

A SysML-based approach for designing an ideal blockchain-based data trading platform

Aydın Elbüz*, Murat Osmanoğlu, Özgür Tanrıöver
Department of Computer Engineering, Faculty of Engineering, Ankara University, 06830, Ankara, Türkiye

Highlights:

- An ideal blockchain-based data trading platform and its features.
- Summary of other studies in the literature and their weaknesses.
- Analyzing the platform and determining the requirements with SysML.

Keywords:

- Blockchain
- Internet of things
- Data trading
- SysML

Article Info:

Research Article
Received: 09.11.2021
Accepted: 19.03.2023

DOI:

10.17341/gazimmfd.1020217

Correspondence:

Author: Aydın Elbüz
e-mail:
aelbuz37@gmail.com
phone: +90 545 561 4297

Graphical/Tabular Abstract

In this study, a blockchain-based data trading platform is proposed where IoT (Internet of Things) data can be marketed. The main purpose of this platform is to allow users to trade data in a reliable and healthy way, so the components of the platform were determined according to these needs and solution methods were presented according to the requirements. As seen in Figure A, the platform has 4 main components: "Registration" component for joining the platform. "Data Record Creation" component for creating data record to be sold. "Trading" component for performing sell and buy operations. "Block Processing" component for operations after the trading. Also, the platform has 3 side components: "Internet of Things" component defines the data source. "Users" component defines the users in the platform. "Blockchain" component defines the database of the platform.

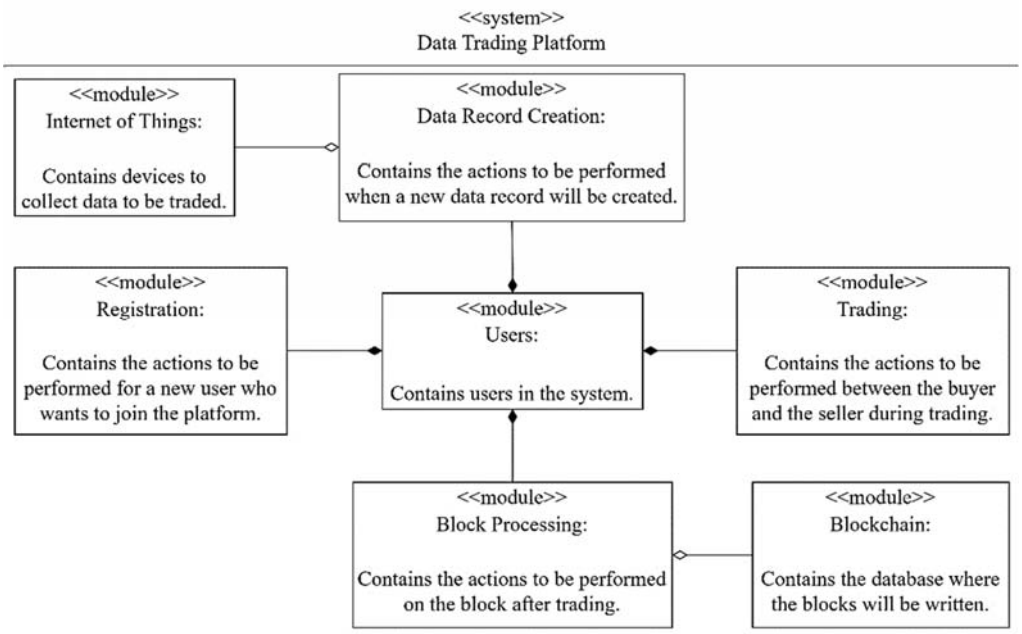


Figure A. General structure of the data trading platform

Purpose: The purpose of this study is to determine the main components and the features of this system and clarify how an ideal blockchain based data trading platform should be.

Theory and Methods: In order to determine how an ideal platform should be, other studies in the literature were analyzed and determined their weaknesses. Based on these studies, the components and the requirements of an ideal system were determined. Then, the relations of these components with each other and how the requirements can be met were explained. Also, SysML was used in order to explain this platform and their components.

Results: The working of this proposed ideal data trading platform is explained through an example scenario. All features are involved and the requirements of the ideal system were met with this flow.

Conclusion: Nowadays, workable data that obtained from IoT is rather substantial and valuable. This situation indicates the need for a trading platform for these data. Studies for this circumstance exist but have some weaknesses. In order to meet the requirements and annihilate the weaknesses, an ideal data trading platform is needed.

Journal of the Faculty of Engineering and Architecture of Gazi University 39:1 (2024) 509-519

Mühendislik Mimarlık Fakültesi Dergisi
Journal of The Faculty of Engineering and Architecture of Gazi University

Elektronik / Online ISSN : 1304 - 4915
Basılı / Printed ISSN : 1300 - 1884

Blok zinciri tabanlı ideal bir veri ticareti platformunun tasarımı için SysML tabanlı bir yaklaşım

Aydın Elbüz*, Murat Osmanoğlu, Özgür Tanrıöver
Ankara Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 06830, Gölbaşı Ankara Türkiye

Ö N E Ç I K A N L A R

- Blok zinciri tabanlı ideal bir veri ticaret platformu ve özellikleri
- Literatürdeki diğer çalışmaların özeti ve eksik yönleri
- Platformun SysML kullanılarak analiz edilmesi ve gereksinimlerin belirlenmesi

Makale Bilgileri
Araştırma Makalesi
Geliş: 09.11.2021
Kabul: 19.03.2023

DOI:
10.17341/gazimmfd.1020217

Anahtar Kelimeler:
Blok zinciri,
nesnelerin interneti,
veri ticareti,
SysML

ÖZ

Nesnelerin interneti (internet of things - IoT), bir ağ üzerinden birbirine bağlanan ve içerisinde algılayıcıların bulunduğu farklı tipteki cihazlar topluluğudur. İlk uygulaması 1982 yılında gerçekleştirilen bu teknoloji; günümüzde özellikle internetin yaygınlaşmasıyla beraber, tanımlama ve izleme teknolojileri, kablolu ve kablosuz algılayıcılar ve dağıtık bilişim sistemleri gibi birçok alanda sıklıkla kullanılmaktadır. Kullanım alanları genişledikçe, bu teknoloji veri toplama amacıyla da değerlendirilmeye başlanmıştır. Diğer yandan, işlenebilir verinin önemli ölçüde kıymet kazandığı bir çağda, nesnelerin interneti yoluyla veri toplamak sadece verinin ilintili olduğu alandaki araştırmacılar için değil, aynı zamanda bu veriden ticari menfaat elde etmek isteyenler için de mühim bir uğraş hâline gelmiştir. Bu durum, bu tür verilerin güvenilir ve sağlıklı bir şekilde pazarlanabilmesi ihtiyacını ortaya çıkarmıştır. Blok zinciri teknolojisi; şeffaflık, kayıtların değiştirilemezliği ve ademi merkeziyetçilik gibi özellikleri dolayısıyla bu ihtiyacın karşılanması noktasında etkili ve güvenli bir araç olarak öne çıkmaktadır. Bu çalışmada SysML diyagramları yardımıyla blok zinciri tabanlı ideal bir veri ticaret platformunun nasıl olması gerektiği irdelenmiştir. Bu doğrultuda önce ilgili platformun bileşenleri belirlenmiş ve bu bileşenler arasındaki ilişkiler analiz edilmiştir. Ayrıca bahsi geçen sistemin güvenli ve etkili bir biçimde çalışabilmesi için ihtiyaç duyulan gereksinimler tanımlanmış; dahası, bu gereksinimlerin nasıl karşılanabileceği örnek bir senaryo üzerinden gösterilmiştir.

A SysML-based approach for designing an ideal blockchain-based data trading platform

H I G H L I G H T S

- An ideal blockchain-based data trading platform and its features
- Summary of other studies in the literature and their weaknesses
- Analyzing the platform and determining the requirements with SysML

Article Info
Research Article
Received: 09.11.2021
Accepted: 19.03.2023

DOI:
10.17341/gazimmfd.1020217

Keywords:
Keywords:
Blockchain,
internet of things,
data trading,
SysML

ABSTRACT

Internet of things (IoT) is a collection of various types of devices that has sensors and connected to each other over a network. This technology was first implemented in 1982 and today, especially with the spread of the internet, it is frequently used in many areas such as identification and monitoring technologies, wired and wireless sensors and distributed information systems. As its usage areas have expanded, this technology has started to be used for data collection purposes. On the other hand, in an era where workable data has gained significant value, collecting data via the IoT has become an important endeavor not only for researchers in the field of data, but also for those who want to gain commercial benefits from this data. This situation has revealed the need to market such data in a reliable and healthy way. Due to its features such as transparency, immutability of records and decentralization, blockchain technology stands out as an effective and safe method to meet this need. In this work, with the help of SysML diagrams, it is examined that how an ideal blockchain-based data trading platform should be. In this direction, first the components of the platform were determined and the relations between these components were analyzed. In addition, the requirements needed for this system to work safely and effectively have been defined. Moreover, how these requirements can be met is demonstrated through an example scenario.

*Sorumlu Yazar/Yazarlar / Corresponding Author/Authors : *aelbuz37@gmail.com, murat.osmanoglu@ankara.edu.tr, tanriover@ankara.edu.tr / Tel: +90 545 561 4297

1. Giriş (Introduction)

Nesnelerin interneti, bir ağ üzerinden birbirine bağlanan ve içerisinde sensörlerin bulunduğu farklı tipteki cihazlar topluluğudur [1]. Uygulama olarak kabul edilebilecek ilk örneği 1982 yılında Carnegie Mellon Üniversitesi'nde gerçekleştirilmiş olmasına rağmen, nesnelerin interneti kavramı ilk defa 1999 yılında Kevin Ashton tarafından kullanılmıştır. Nesnelerin internetindeki cihazların her biri benzersiz bir kimliğe sahip olup, ağdaki diğer cihazlarla haberleşebilmekte veya kontrol edilebilmektedir.

Bu teknoloji günlük yaşamda akıllı ev ve şehir sistemlerinde sıklıkla kullanılmaktadır. Bir yandan ortamdaki cihazların uzaktan kontrolüne imkân verirken diğer yandan da cihazların ortamın durumunu okumasını ve kullanıcıya bilgi göndermesini sağlamaktadır. Tarım sektöründe tarlaların sıcaklık, nem, rüzgâr ve yağış miktarı gibi kritik verilerini kullanıcıya göndererek ürünlerin daha düşük maliyette daha kaliteli şekilde yetişmelerine yardımcı olmaktadır. Sağlık sektöründe ise akıllı saatler ve benzeri sensörler yardımıyla hastaların kalp atış hızı, tansiyon gibi kritik değerlerinin doktorlar tarafından takip edilmesini kolaylaştırmakta ve sağlık hizmetlerindeki kalitenin geliştirilmesine ciddi katkı sağlamaktadır.

Nesnelerin interneti teknolojisinin kullanım alanları genişledikçe, bu cihazlar veri toplama amacıyla da kullanılmaya başlanmıştır. Toplanan veriler, örneğin sağlık sektöründe daha etkin ve hızlı uygulanabilen tedavilerin bulunmasını amaçlayan araştırmalarda kullanılabileceği gibi tarımsal ürünlerin rekoltesini artırmaya yönelik çalışmalarda da kullanılabilmektedir [2]. Dolayısıyla işlenebilir verinin önemli ölçüde kıymet kazandığı bir çağda, nesnelerin interneti yoluyla veri toplamak sadece verinin ilintili olduğu alandaki araştırmacılar için değil, aynı zamanda bu veriden ticari menfaat elde etmek isteyenler için de mühim bir uğraş hâline gelmiştir. Bu durum, bu tür verilerin güvenilir ve sağlıklı bir şekilde pazarlanabilmesi ihtiyacını ortaya çıkarmıştır.

Blok zinciri teknolojisi, merkezi olmayışı, verilerin şeffaf ve değiştirilemez bir şekilde kaydedilebilmesine olanak sağlaması gibi özellikleri dolayısıyla bu ihtiyacın karşılanması konusunda önemli ve etkin bir araç olarak kullanılabilir. Blok zinciri, dağıtık kayıt defterini gerçekleyerek işlemleri kullanıcılara açık ve merkezi olmayan bir sistemde depolamaya izin veren yeni bir teknolojidir. Blok zincirinde işlemler sistemdeki kullanıcılar tarafından onaylandıktan sonra değiştirilemez ve silinemez bir biçimde dağıtık kayıt defterine eklenirler. Blok zinciri salt okunur bir veri tabanı sistemi olup, hatalı veya sahte bir işlemin zincire yazılmasına izin vermez. Güvenilirliği, şeffaflığı ve veri değiştirilemezliğini sağlayan bu sistemin ilk ortaya çıkışı 1991 yılına dayansa da, 2008 yılında Satoshi Nakamoto'nun ortaya attığı eşler arası elektronik para sistemi Bitcoin ile bir anda popülerlik kazanmıştır. Günümüzde blok zinciri teknolojisi; tarımdan [3] eğitime [4], sağlıktan [5] sigortacılığa [6] kadar birçok farklı alanda güncel problemlerin çözümünde etkin bir biçimde kullanılmaktadır.

Blok zinciri teknolojisi yukarıda bahsi geçen problem için etkin ve güvenilir bir çözüm sunsa da, bazı riskleri de beraberinde getirmektedir. Örneğin kötü niyetli bir satıcı, takas sırasında alıcıdan parayı aldıktan sonra veriyi göndermeyebilir veya kullanılamaz bir veri gönderebilir. Aynı şekilde kötü niyetli bir alıcı da, satıcıdan veriyi aldıktan sonra üzerinde mutabık kalınan parayı göndermeyebilir. Ayrıca her ne kadar merkezi bir otoritenin olmayışı blok zincirini tek bir hata noktası (single point of failure) probleminden sakındırsa da, yine kötü niyetli bir otorite platformda gerçekleştirilen alışveriş işlemleri üzerinde değişiklikler yaparak alışverişin taraflarının mağdur olmasına sebebiyet verebilir. Dolayısıyla bu ve benzeri durumlardan kaçınmak ve ilgili taraflara güvenilir bir ticaret ortamı sunmak için, sistemin ihtiyaç duyduğu bütün bileşenlerin dikkatli ve titiz bir şekilde tanımlanması ve analiz edilmesi gerekmektedir. Ayrıca bu bileşenlerin sağlıklı ve verimli bir şekilde çalışabilmeleri için ihtiyaç duyulan gereksinimler tespit edilmeli ve bu gereksinimlerin hangi koşullar altında karşılandığı belirlenmelidir.

1.1. Blok Zinciri (Blockchain)

Blok zinciri, temeli dağıtık kayıt defterine dayanan bir kayıt ve depolama sistemidir. Sistem, işlem kayıtlarını içeren bloklardan oluşur ve bu blokların zincir şeklinde arka arkaya sıralanmasından dolayı bu isimle anılmaktadır. Bu bloklar, sisteme eklenme sırasına göre sıralıdır ve art arda gelen her iki blok arasında bir ilişki bulunmaktadır: her blok, kendinden önceki bloğun özet değerini barındırmaktadır. Bu özet değeri, kriptografik özet fonksiyonları ile hesaplanmaktadır ve blokların değişmediğini garantilemektedir. Zincirdeki ilk bloğa başlangıç bloğu (genesis block) adı verilir ve devamındaki blokların zincire eklenme işlemi uzlaşma algoritmaları ile gerçekleştirilir. Uzlaşma algoritmaları sayesinde her kullanıcı zincirin aynı kopyasını barındırmış olur ve dolayısıyla yerel kopyaya eklenen hatalı bir değişiklik, sistemdeki diğer kullanıcılar tarafından onaylanmayacağı için asıl zincire eklenmez. Bu ve benzeri durumlara karşı veri tabanının güvenliği kriptografik özet fonksiyonları ve dijital imzalarla sağlanmaktadır.

Blok zincirleri, erişim durumuna göre izinli (permissioned) ve izinsiz (permissionless) olmak üzere ikiye ayrılmaktadır. İzinsiz blok zincirleri çoğunlukla kripto para sistemlerinde kullanılmakta olup herhangi bir izin istemeden herkesin katılabileceği ağlardır. İşlemler ağdaki herhangi bir kullanıcı tarafından onaylanabilmekte ve sistemin güvenliği de yine bu kullanıcılar tarafından sağlanmaktadır. Öte yandan izinli blok zincirlerinde bir erişim kontrolü bulunmakta olup, sadece otoriteler tarafından izin verilen kullanıcılar sisteme katılabilmektedir. Bununla birlikte işlemler de sadece sistemde izin verilen kullanıcılar tarafından onaylanabilmekte ve bu kullanıcılar ağ sahibi tarafından kontrol edilebilmektedir. Geliştirilen sistemin ihtiyacına göre blok zinciri izinli veya izinsiz olabilmektedir.

Blok zinciri anonimliği sağlamakta olup, hiçbir kullanıcı bir işlemi gerçek kimlik bilgileri ile gerçekleştirmez; bunun yerine sistem tarafından üretilmiş bir sayısal kimlik kullanır. Bununla birlikte blokların yazımı sırasında uzlaşma algoritmalarının kullanılması, zincirdeki verilerin bütünlüğünü garantilemektedir. Dağıtık olması sayesinde de oluşabilecek herhangi bir hatada sistemin tamamen çökmesi önlenmektedir.

1.2. SysML (SysML)

SysML, geliştirilecek bir sistemin belirli seviyelerdeki tasarımlarının ve analizlerinin yapılabilmesi için kullanıcılara çeşitli diyagram yapıları sunan ve bu sayede sistemin detaylı olarak irdelenebilmesine olanak sağlayan bir tasarım dilidir. Bu dilde sistem içerisindeki yapılarda kullanılacak elemanlar blok veya modül olarak isimlendirilmekte olup, bu blok veya modüller birbirlerine yönlü ve ilişkili oklarla bağlanmakta ve birbirlerine olan ilişkinin kuvveti okun türüne ve yönüne göre değişiklik göstermektedir. SysML, içerisinde barındırdığı farklı diyagramlar ile geliştirilecek sistemin bileşenlerine çeşitli açılardan bakılmasına imkân tanımaktadır.

Blok tanımı (block defitinion) diyagramı, sistem ve sistemin alt bileşenleri ile bunlar arasındaki hiyerarşiyi belirten diyagramlardır. Sistem alt bileşenlerini ve bu bileşenlerin içeriklerini tanımlayan diyagramlar ise iç blok (internal block) diyagramı olarak tanımlanır. Kullanım senaryosu (use-case) diyagramı, sistemi kullanacak olan son

kullanıcının sistem üzerinde yapabileceği işlemleri ve hareketleri tanımlayan diyagramlardır. Sistemin ve sistemin alt bileşenlerinin kendi içerisindeki fonksiyonlarını ve davranışlarını tanımlayan diyagramlar ise faaliyet (activity) diyagramı olarak isimlendirilmektedir. Geliştirilecek sistemin ihtiyaçlarını belirlemek ve bu ihtiyaçların hangi modüller veya bileşenlerle karşılanacağına karar vermek için kullanılan diyagram ise gereksinim (requirement) diyagramıdır. Bunların haricinde kullanılan başka diyagramlar olsa da genel çerçevede bir sistemin tasarımının yapılabilmesi için yukarıda belirtilen diyagram tipleri sıklıkla kullanılmaktadır.

1.3. Literatür Araştırması (Literature Research)

Günümüzde IoT cihazlarının büyük bir kısmı sensörlerden oluşmakta ve bu sensörler sayesinde veri toplanmasına olanak sağlanmaktadır. Tarım sektöründe ortam, sağlık sektöründe hasta bilgileri vb. olmak üzere birçok sektör tarafından toplanan bu veriler; ilgili kişilerce doğrudan kullanabileceği gibi araştırmacılar tarafından iş süreçlerinin geliştirilmesini ve maliyetlerin düşürülmesini amaçlayan çalışmalarda da kullanılabilmektedir. Dolayısıyla bu tür verilerin doğrudan kullanımının yanı sıra depolanıp pazarlanabilmesine olanak sağlayacak platformlara da ihtiyaç vardır. Bu tip verilerin pazarlanması için Tzianos vd. [7] tarafından önerilen izinsiz blok zinciri tabanlı sistemde; satıcılar ellerindeki sensörlerin bilgilerini, alıcılar da istedikleri veri tipini market üzerinden yayınlayabilmektedir. Pazarlama işlemi, istenen sensörün verilerine belirli bir süre ulaşabilme hakkı tanımaktadır. Alıcıların satın aldığı sensöre ait veriler bir depolama alanına belirli bir formatta şifreli olarak kaydedilmektedir. İstenildiği durumda bu alan üzerinden veri anahtarları vasıtasıyla şifresi açılarak verilere ulaşılabilmektedir. Önerilen bu sistem izinsiz bir blok zinciri olmasına rağmen kullanıcıların bu sisteme nasıl erişebilecekleri veya katılım sağlayabilecekleri belirtilmemiştir. Ayrıca sistem içerisinde veriler şifreli olarak paylaşılsa dahi kötü niyetli bir satıcının, alıcıya kullanılamaz bir veri veya hatalı veri anahtarı gönderme ihtimali göz ardı edilmiştir.

Manzoor vd. [8] de benzer bir sistemi Ethereum tabanlı izinli blok zincirini kullanarak oluşturmuşlar ve veri kaydı esnasında verileri ayrı bir depolama alanı olarak bulut depolamaya kaydetmişlerdir. Bunun yanı sıra verileri satıcının anahtarı ile şifreleyerek veri güvenliğini de sağlamışlardır. Verilerin satışı gerçekleştirildiğinde ise bu şifre açılarak bu sefer alıcının açık anahtarına göre şifreleme yapılmış ve verilere bulut depolama üzerinden alıcının kendi kapalı anahtarı ile erişebilmesi sağlanmıştır. Sistem izinli blok zinciri kullanılarak tasarlanmış olmasına rağmen, çalışmada kimlerin hangi şartlar altında sisteme katılabileceği ve sistemdeki otoritelerin nasıl belirlendiği açıklanmamıştır.

Papadodimas vd. [9] ise sensör verisi olarak hava durumu bilgilerinin pazarlanabildiği izinli blok zinciri kullanan ve yukarıda bahsi geçen yapılara ek olarak, alışveriş esnasında kullanılabilecek sistem içi yeni bir para birimi öneren bir platform sunmuşlardır. Ethereum altyapısı kullanıldığı için sistem, sistem içi oluşturulan para ile Ethereum platformunda kullanılan Ether arasında değişiklik yapılabilmesini de desteklemektedir. Ancak yukarıda anlatılan sisteme benzer şekilde, burada da kullanıcı ve otoritelerin nasıl belirlendiğinden bahsedilmemiştir.

Sensör haricinde, başta akıllı telefonlar olmak üzere günlük hayatta kullanılan cihaz ve araçlarda da IoT teknolojisi kullanılabilmektedir. Bu doğrultuda An vd. [10] mobil cihazlardan elde edilen kitle yoğunluğu (crowdsensing) verilerinin pazarlanabildiği bir sistem önermişlerdir. Sistemde akıllı sözleşme tabanlı araçlar alıcılardan gelen talepleri satıcılara ileterek satıcılardan fiyat teklifi almaktadır. Alınan bu teklifler arasından, ters açık artırma yöntemi ile uygun satıcılar belirlenmekte ve alıcılar ile iletişime geçirilmektedir. Satın alınan şifreli veriler bulut sunucuları üzerinden, şifreler de akıllı sözleşme tabanlı yardımcılar tarafından güvenli bir yol ile alıcılara gönderilmektedir. Lakin önerilen bu sistem alıcıların verilerin kalitesini veya kullanılabilirliğini belirlemesine olanak tanımamaktadır. Bu durum, alıcıların kullanılamaz veriler alabilme ihtimalini ortaya çıkarmaktadır.

Benzer bir sistemi Chen vd. [11] de araçların interneti (internet of vehicles) ağına bağlı cihazlardan elde edilen veriler için önermişlerdir. Alıcılar veri ihtiyaçlarını aracılara iletmekte, aracılar ise bu ihtiyaçları satıcılara ileterek fiyat teklifi almakta ve uygun fiyatlı teklifi tekrar alıcıya bildirmektedir. Aracılar akıllı sözleşme tabanlı olup, sadece veri ihtiyacının ve fiyat teklifinin karşı tarafa iletilmesinden sorumludur. Dolayısıyla paranın ve verinin takasında herhangi bir aracı taraf bulunmamakta, alıcı veriyi aldıktan sonra parayı direkt olarak satıcıya göndermektedir Alışverişin bu şekilde tasarlanmış olması alıcının veriyi aldıktan sonra parayı göndermeme ihtimalini doğurmaktadır. Ayrıca bu sistemde de verilerin kullanılabilirliğini ve kalitesini belirleyen herhangi bir mekanizmadan bahsedilmemiştir.

IoT verilerinin satışı sırasında hem alıcının hem de satıcının haklarının korunabilmesi adına verinin analizi ve fiyatlandırılması güvenli bir alışveriş için kritik bir rol oynamaktadır. Özellikle alıcının işe yarar bir veri alabilmesi ve mağdur olmaması için, alışveriş öncesinde veya alışveriş esnasında verinin analiz edilebilmesi/incelenmesine olanak sağlanması gerekmektedir. Bu doğrultuda Kiyomoto ve Fukushima [12] taraflara adil pazarlama olanağı sunan bir sistem önermişlerdir. Sistem, veri almak isteyen veri analistleri ile bu verileri analistlere gönderecek olan veri aracıları arasında adil bir fiyatlandırma yapılmasını sağlamaktadır. Aracılar, ellerindeki verileri şifreli bir biçimde depolama alanına yüklemekte ve yüklenen bu veriler parçalara ayrılarak her bir parçanın doğrulama etiketi hesaplanmakta ve kaydedilmektedir. Analistler, almak istedikleri verileri analiz edebilmek maksadıyla veri setinden görmek istedikleri rastgele bir kaydı aracıdan istemekte ve gelen parçanın doğruluğunu, depolama alanından gelen ilgili doğrulama etiketi vasıtasıyla kontrol etmektedir. Ayrıca verinin fiyatlandırılması aşamasına geçilebilmesi, ancak bu işlemin belirli bir sayıda (en fazla veri setindeki kayıt sayısı kadar olmak üzere) yapılması sonucunda gerçekleştirilmektedir. Önerilen bu sistemde verinin fiyatlandırılması ve alıcı tarafına gönderilmesi aşamalarından bahsedilmiş, ancak veri karşılığında gönderilecek paranın alıcıya nasıl ve ne şekilde iletileceğine değinilmemiştir.

Elbüz vd. [13], verilerin alıcılar tarafından incelenebilmesine olanak sağlayan ve izinsiz blok zinciri kullanan bir ticaret platformu önermişlerdir. Sistemde satıcılar, verilerini anlamlı küçük veri setlerine bölmekte ve bu veri setleri üzerinden bir özet değeri hesaplayarak blok zincirine yüklemektedir. Alıcılar ise satın almak istedikleri veriyi oluşturan veri setleri arasından rastgele bir sayı seçmekte ve bu sayıya denk gelen veri setini alıcıdan alıp inceleyebilmektedirler. Alışveriş işlemi, satın alınacak verinin özet değerinin blok zincirindeki özet değeriyle aynı olduğu durumda gerçekleştirilmekte ve bu sayede verinin değiştirilmediği garantilenmektedir. Kiyomoto ve Fukushima [12]'nın çalışmasından farklı olarak bu çalışmada veriler herhangi bir depolama alanına yüklenmemekte, bütün veriler satıcıların kendi depolama sistemlerinde bulunmaktadır. Ayrıca satılacak verinin fiyatlandırılmasına dair de herhangi bir işlem yapılmamaktadır. Bununla birlikte bu çalışmada, kötü niyetli oyunculara karşı platformun nasıl bir koruma önerdiğini irdeleyen detaylı bir güvenlik analizi yapılmamıştır. Diğer yandan Dai vd. [14] ise alıcının, almak istediği veriyi analiz algoritmaları vasıtasıyla ölçebildiği bir sistem önermişlerdir. Bu sistemde alıcı elindeki analiz algoritmalarını, satıcı

da elindeki veriyi daha önceden belirlenmiş güvenilir kullanıcılara göndermektedir. Bu kullanıcılar analiz algoritmaları üzerinden elde ettikleri sonuçları tekrar alıcıya göndererek alıcının veri hakkında bilgi sahibi olmasını sağlamaktadırlar. Bu sistem alıcıya satın almadan önce veriyi inceleme fırsatı sunsa da, alışveriş esnasında para ve veri takasının nasıl yapılacağından bahsedilmemiştir. Ayrıca, verinin analiz için gönderildiği aracılar güvenilir kabul edilmiş ve kötü niyetli aracıların sisteme verebileceği zararlar irdelenmemiştir.

Bunlara ek olarak, Guan vd. [15] büyük verilerin ve bu verilerin istatistiksel bilgilerinin pazarlanabilmesini sağlayan bir sistem önermiştir. Sistemde gerçek zamanlı sağlık verileri kullanılmıştır. Sistem içerisinde veriler işlenmeden önce küçük parçalara ayrılmış ve her bir parçanın özet değeri hesaplanarak verilerin değiştirilmesinin önüne geçilmiştir. Ayrıca bu yolla alıcıların, satın aldıkları verileri özet değerleri vasıtasıyla kontrol edebilmelerine de imkân tanınmıştır. Ancak sistem, alıcılara platforma yüklenen verilerin içeriği hakkında herhangi bir bilgi sunmamış olup; bu durum alıcının platformdaki bir verinin içeriğini ve genel bilgilerini öğrenememesinden başlayıp satın almak istediği veriyi platformda bulamamasına kadar giden bir sürece neden olabilmektedir.

Huang vd. [16], IoT verilerinin pazarlanabilmesini sağlayan Ethereum blok zinciri tabanlı katmanlı bir mimari önermişler ve verileri işlemlerin kaydedildiği blok zinciri ile aynı katman içerisinde bulunan farklı bir depolama sistemine (bulut depolama, veri tabanı vb.) kaydederek performansın artırılmasını amaçlamışlardır. Bununla birlikte veri sahiplerinin, platforma veri yükledikleri sırada veriye ait üst bilgilerin de eklenmesini sağlayarak alıcıların veri hakkında bilgi sahibi olmalarını da sağlamışlardır. Ancak önerilen bu sistemde verilerin bir depolama alanına kaydedilmesine karşın, veri üzerinde herhangi bir şifreleme veya değiştirilemezlik işlemi gerçekleştirilmemiş olup; bu durum verileri, üzerinde değişiklik yapmaya açık hâle getirmiştir.

Sabounchi vd. [17] alıcılara, almak istediği verinin özelliklerini ve ödemek istediği miktarı içeren teklifler oluşturarak bu teklifleri ilgili satıcılara iletebilmesine olanak sağlayan bir sistem önermişlerdir. İletilen bu teklifler sonrasında akıllı sözleşmeler vasıtasıyla satıcın seçtiği tekliflerden biri üzerinden satış işlemi gerçekleştirilmektedir. Her ne kadar veri ve para transferi akıllı sözleşmeler vasıtasıyla gerçekleştirilse de, veri üzerinde herhangi bir şifreleme işlemi yapılmamış; bununla birlikte alıcının da almak istediği veriyi kontrol edebileceği bir sistem sunulmamıştır. Önerilen sistem her ne kadar akıllı sözleşmeler üzerinden taraflara güvenli bir alışveriş vadediyor olsa da, verinin değiştirilemezliğini garantilememekte ve alıcıya aldığı veriyi kontrol edebilme olanağı sunmamaktadır.

Yukarıda bahsedilen platformlardan farklı olarak Wang vd. [18] iki farklı blok zinciri kullanan bir veri paylaşım modeli önermişlerdir. Önerilen modelde blok zincirlerinden biri verilerin tamamını depolamada, diğeri ise yapılan işlemlerin saklanmasında kullanmıştır. Veriler öncelikle küçük parçalara ayrılarak her bir parçanın özet değeri hesaplanmış, ardından bu parçalar şifrelenerek kendi özet değerleri ile birlikte veri blokları hâlinde verilerin depolandığı blok zincirine kaydedilmiştir. Verilerin parçalara ayrılarak özet değerlerinin hesaplanması, verilerin değiştirilemez bir biçimde depolanmasına olanak sağlamış ve sistemin güvenilirliğini artırmıştır. Ancak önerilen sistemde veriler blok zincirinde tutulduğu için veri sayısı arttıkça blok zincirinin boyutunun da artması kaçınılmaz olacaktır ve bu durum, ileriki zamanlarda depolama problemlerine yol açacaktır.

Zheng vd. [19] ise başarılı alışveriş işlemleri sonrasında veri sahibine ödül verilmesini sağlayan Ethereum tabanlı kapalı bir blok zinciri sistemi önermişlerdir. Önerilen bu sistemde alıcı taraf veri ihtiyaçlarını yayınlamakta ve yukarıda bahsedilen diğer sistemlerden farklı olarak veri dağıtıcıları olarak adlandırılan kullanıcılar bu ihtiyaçlar doğrultusunda veri sahiplerinden aldıkları verileri alıcılara iletmektedir. Alıcı, satın aldığı verinin kullanım bilgilerini zincire kaydetmekte, bu sayede verilerin kalitesinin artmasına katkı sağlamaktadır. Bununla birlikte sistem, alıcının satın aldığı verinin kalitesine ve miktarına göre veri sağlayıcısına ödül vermektedir. Her ne kadar bu işlem sırasında verilebilecek puanın bir alt ve üst sınırı olsa da, satıcının alıcı ile anlaşıp yüksek puan verme ihtimali göz ardı edilmiştir. Ayrıca kötü niyetli bir alıcı ve satıcının karşılıklı anlaşma ile sistemi suistimal edecek derecede puanlama yapması, sistemdeki diğer alıcıların satıcılar hakkında hatalı bilgilenmelerine; bunun devamında da kötü niyetli bir satıcıya denk gelerek olası kötü senaryolar sonucunda mağdur olabilmelerine sebebiyet verebilir ve sisteme olan güvenleri sarsılabilir.

1.4. Çalışmanın Katkısı (Contribution)

Yukarıda bahsedilen veri ticaret sistemlerinin hepsinin kendi içerisinde zayıf veya eksik bir yönü bulunmakta olup, bu eksiklikler veya zayıflıklar dolayısıyla hiçbiri ideal bir sistem olarak tanımlanamamaktadır. Bu noktada öncelikli olarak yapılması gereken blok zinciri tabanlı ideal bir veri ticareti platformunun tanımlanması olacaktır. Bu doğrultuda platformu oluşturan bütün bileşenlerin belirlenmesi, bu bileşenlerin sağlıklı ve güvenli bir şekilde çalışabilmesi için ihtiyaç duyulan gereksinimlerin tespit edilmesi ve tespit edilen gereksinimlerin hangi koşullar altında karşılandığı analiz edilmelidir. Bu noktada SysML (The Systems Modeling Language) etkin ve fonksiyonel bir araç olarak değerlendirilebilir.

SysML, sistemlerin ve bu sistemlere ait alt bileşenlerin tasarımının ve analizinin yapılmasını sağlayan bir modelleme yöntemidir. Yöntem, UML (Unified Modeling Language)'nin bir uzantısı olarak 2007 yılında standart bir modelleme dili olarak literatüre sunulmuştur. SysML sayesinde, tasarlanan sistemlerin ve sistemlerin iç yapısının paydaşlar arasında kolaylıkla anlaşılabilmesi sağlanmış ve sistem geliştirme yaşam döngüsünde karşılaşılabilecek hataların ve risklerin önceden görülmesi mümkün kılınmıştır.

Bu çalışmada SysML diyagramları yardımıyla blok zinciri tabanlı ideal bir veri ticaret platformunun nasıl olması gerektiği irdelenmiştir. Bu doğrultuda önce ilgili platformun bileşenleri belirlenmiş ve bu bileşenler arasındaki ilişkiler analiz edilmiştir. Ayrıca bahsi geçen sistemin güvenli ve etkili bir biçimde çalışabilmesi için ihtiyaç duyulan gereksinimler tanımlanmış ve bu gereksinimlerle platformun bileşenleri arasındaki irtibat irdelenmiştir. Dahası örnek bir senaryo üzerinden bu gereksinimlerin nasıl karşılanabileceği gösterilmiştir.

2. Blok Zinciri Tabanlı Ticaret Platformu (Blockchain Based Trading Platform)

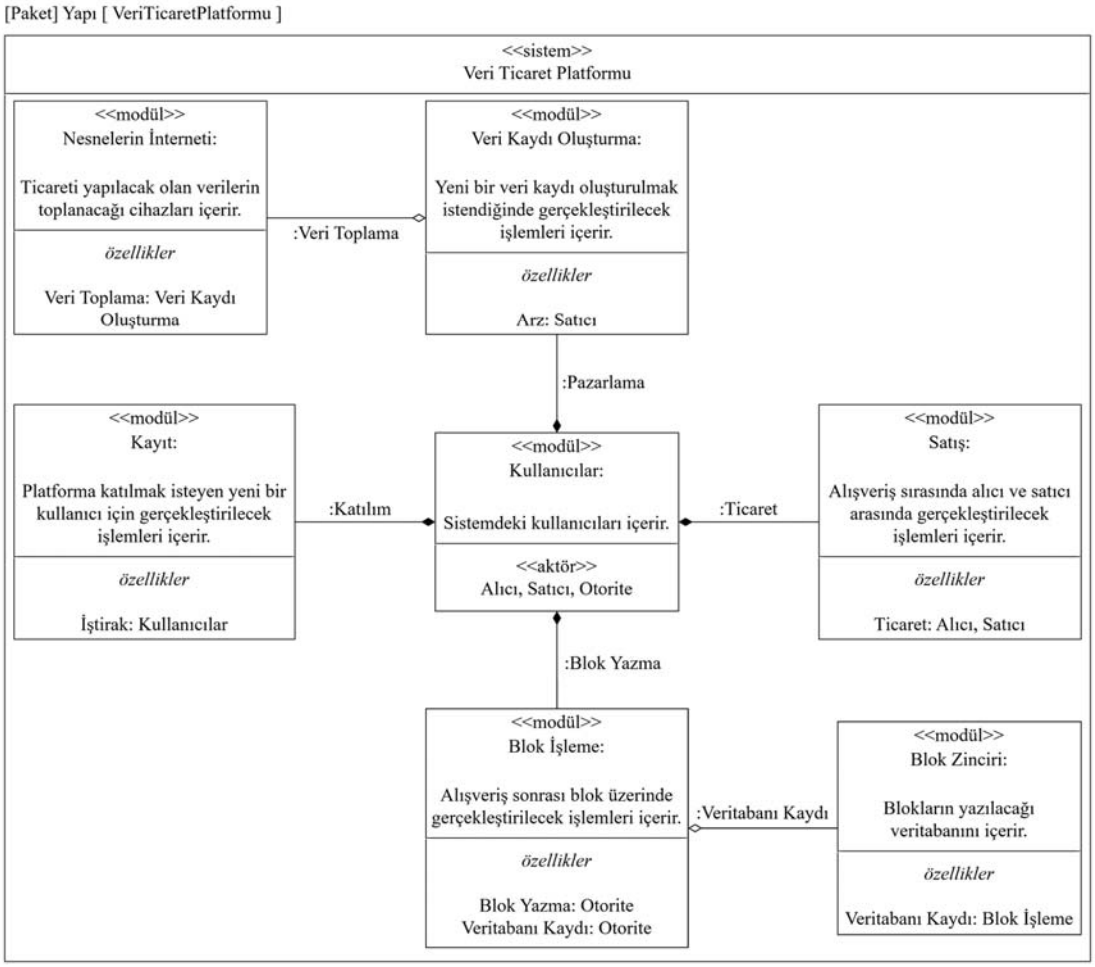
Bu bölümde, blok zinciri tabanlı veri ticaret platformunun SysML diyagramları yardımıyla detaylı açıklaması yapılacaktır. Modelimizde her bir bileşen ayrı bir modül olarak ele alınacak ve bileşenler arasındaki ilişkiler oklar yardımıyla belirtilecektir. Şekil 1'de de gösterildiği gibi blok zinciri tabanlı ticaret platformu; *Kullanıcılar*, *Kayıt*, *Nesnelerin İnterneti*, *Veri Kaydı Oluşturma*, *Satış*, *Blok İşleme* ve *Blok Zinciri* olarak adlandırılan 7 farklı modülden oluşmaktadır. *Kullanıcılar* modülü platform içerisinde yer alacak rolleri belirlemekte olup alıcı, satıcı ve otorite olmak üzere 3 farklı rol içermektedir. Satıcılar, *Nesnelerin İnterneti* modülünden elde ettikleri verileri platform üzerinden pazarlayan ve satan kullanıcılardır. Alıcılar, platform üzerinden *Nesnelerin İnterneti* yoluyla toplanan verileri satın almak isteyen kullanıcılardır. Otoriteler ise, platformda paylaşılan işlemleri toplayan ve blok zincirine kaydeden kullanıcılardır.

2.1. Kayıt (Registration)

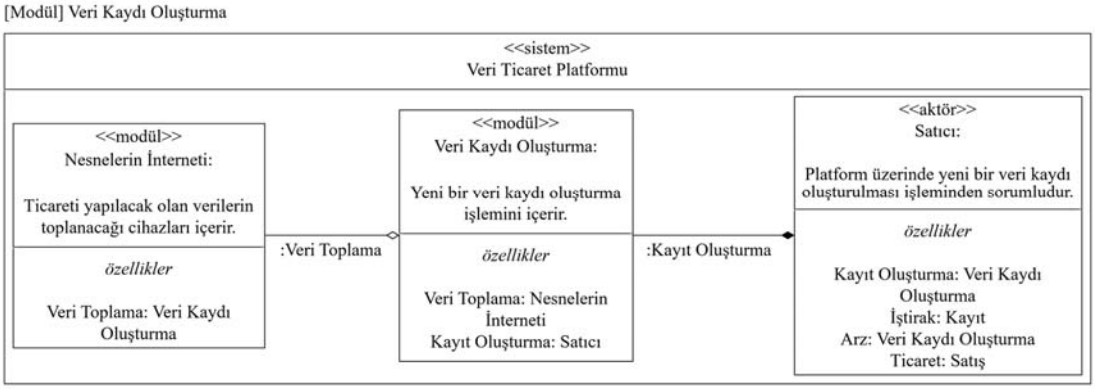
Platform içerisinde alıcı, satıcı veya otorite olarak yer alacak her bir kullanıcının öncelikle *Kayıt* modülü üzerinden platforma kaydolması gerekmektedir. Bölüm 1'de de belirtildiği gibi blok zincirleri izinli ve izinsiz olmak üzere ikiye ayrılmakta olup; izinsiz blok zincirlerinde kullanıcılara kayıt için herhangi bir şart koşulmazken, izinli blok zincirlerinde sadece otoriteler tarafından izin verilen kullanıcılar sisteme kayıt olabilmektedir. Bu çalışmada, platformu izinsiz blok zinciri üzerine inşa edilmiş bir yapı olarak ele alıyoruz. Platform izinli blok zinciri kullanılarak hayata geçirilecekse bu modülün daha dikkatli ve detaylı tasarlanması gerekmektedir.

2.2. Veri Kaydı Oluşturma (Data Record Creation)

Satıcıların platform içerisinde veri satışı gerçekleştirebilmeleri için, öncelikli olarak ilgili verilerle alakalı veri kaydı oluşturmaları gerekmektedir. Bu doğrultuda satıcılar, *Nesnelerin İnterneti* modülü üzerinden elde ettikleri IoT verileri için *Veri Kaydı Oluşturma* modülü yoluyla, alıcıların veri ile ilgili gerekli bilgileri bulabileceği bir veri



Şekil 1. Platformun genel yapısı (General structure of the platform)



Şekil 2. "Veri kaydı oluşturma" modülü ("Data record creation" module)

kaydı oluştururlar (Şekil 2). Bu veri kayıtları ilgili verilerle alakalı gereken açıklamaları içermesinin yanında; ihtiyaca yönelik, örneğin Aydın vd. [13]'de olduğu gibi güvenli bir alışveriş için gerekli olan ekstra bilgiler de içerebilmektedir.

2.3. Veri Alışverişi (Data Trading)

Alıcılar *Veri Kaydı Oluşturma* modülü üzerinden platforma kaydedilen verilerden birini satın almak istediklerinde, önce *Satış* modülü vasıtasıyla ilgili satıcı ile irtibata geçerler. Taraflar alışverişin şartları üzerinde uzlaşmaya varırlarsa, Şekil 3'te de görüldüğü gibi, yine aynı modül üzerinden ilgili verinin ve uzlaşılan paranın takası gerçekleştirilir.

2.4. Blok İşleme (Block Processing)

Şekil 4'te resmedildiği gibi, tasarladığımız modelde platformda paylaşılan işlemler periyodik olarak *Uzlaşı* modülü üzerinden belirlenmiş otoritelerce toplanarak yeni bloklara yazılacak ve oluşturulan bu yeni bloklar platforma kayıtlı otoritelerin onayıyla zincire eklenecektir. Biraz detaylandıracak olursak; bu aşamada, önce *Uzlaşı* modülü yoluyla bloğu oluşturacak lider belirlenir. Lider belirleme süreci platformdaki otoritelerin mutabık kaldığı belirli bir uzlaşı algoritması üzerinden yürütülmektedir. Uzlaşı algoritması üzerinden belirlenen lider, ilgili periyot esnasında platformda paylaşılmış olan işlemleri içeren yeni bir blok oluşturur. Sonrasında lider yeni bloğu platformdaki diğer otoritelerle paylaşır ve yine uzlaşı modülü üzerinden diğer otoritelerce onaylanan bu blok kriptografik özet fonksiyonları yardımıyla değiştirilemez bir şekilde zincire eklenir.

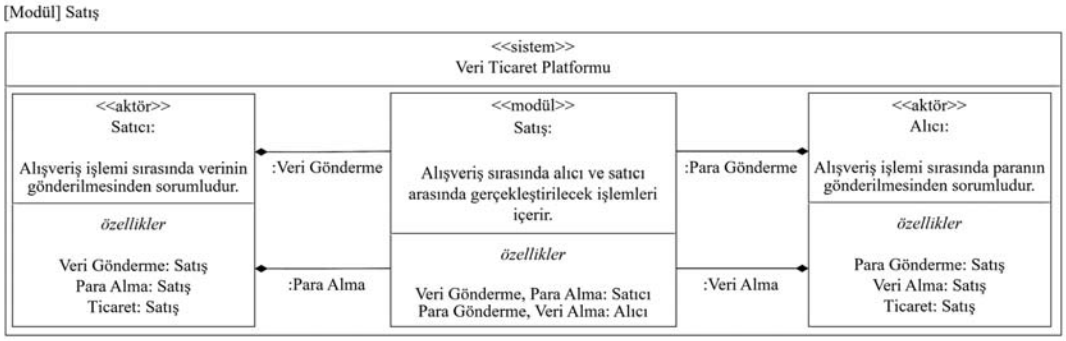
2.5. Gereksinimler (Requirements)

Bu bölümde platformun doğru ve sorunsuz bir şekilde idame ettirilebilmesi için ihtiyaç duyulan gereksinimler tartışılacaktır. Karşılanması gereken bu gereksinimler Şekil 5'te bulunan gereksinim diyagramında gösterilmektedir. Diyagramda gereksinimler ve ilgili modüller arasındaki ilişki standart yönlü kesikli çizgiler vasıtasıyla belirtilmiştir. Bir sonraki bölümde bu gereksinimlerin nasıl karşılanabileceği örnek bir senaryo üzerinden ele alınacaktır.

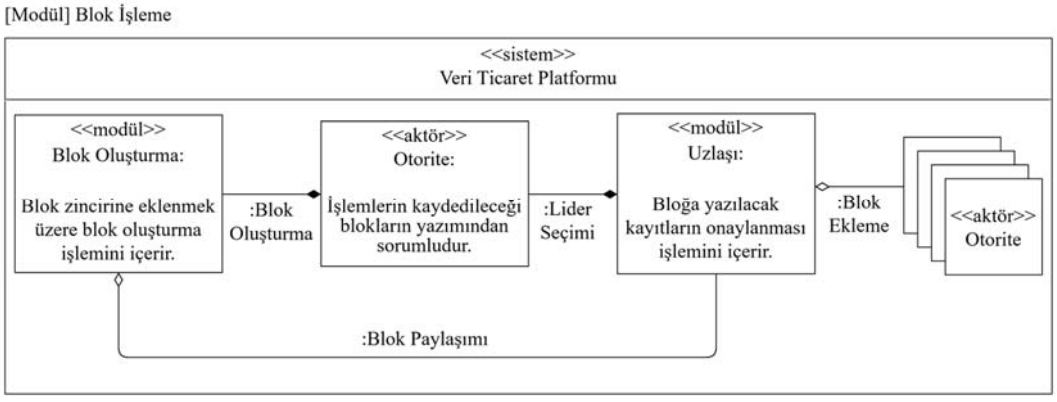
Satışı yapılacak olan veriler platform içerisinde orijinal hâlleriyle tutulursa, sistem şeffaf olduğu için sistemdeki kullanıcılar para ödemeksizin bu verilere erişebilirler. Bundan dolayı verilerin sistem içerisinde gizli bir şekilde tutulması gerekmektedir. Bununla birlikte, veri kaydı oluşturulurken verilerin platformda daha rahat taranabilmesi ve alıcıların satın almak istedikleri verileri kolayca değerlendirebilmesi için, veriyle alakalı bir üst bilginin platformda paylaşılması gerekmektedir.

Kötü niyetli satıcıların, alıcıları kandırmak amacıyla platforma işe yaramaz veriler yükleme ihtimali bulunmaktadır. Bundan dolayı sistemin alıcılara, veri satın almadan önce bu verileri test edebilme imkânı sunması gerekmektedir. Bunun yanı sıra kötü niyetli bir satıcı, satış işlemi sırasında platforma yüklediği veri üzerinde değişiklik yaparak alıcının mağdur olmasına sebep olabilir. Dolayısıyla bu noktada veri bütünlüğünün sağlanması gerekmektedir. Diğer bir ifadeyle, bir alıcının satın almak istediği verinin, başlangıçta platforma yüklenen veri ile aynı veri olduğunun ve üzerinde herhangi bir değişiklik yapılmadığının garantilenmesi gerekmektedir. Ayrıca, alıcı gerekli ücreti ödedikten sonra verinin tamamını; benzer şekilde satıcı da verinin tamamını alıcıya gönderdikten sonra paranın tamamını güvenilir ve sorunsuz bir şekilde alabilmelidir.

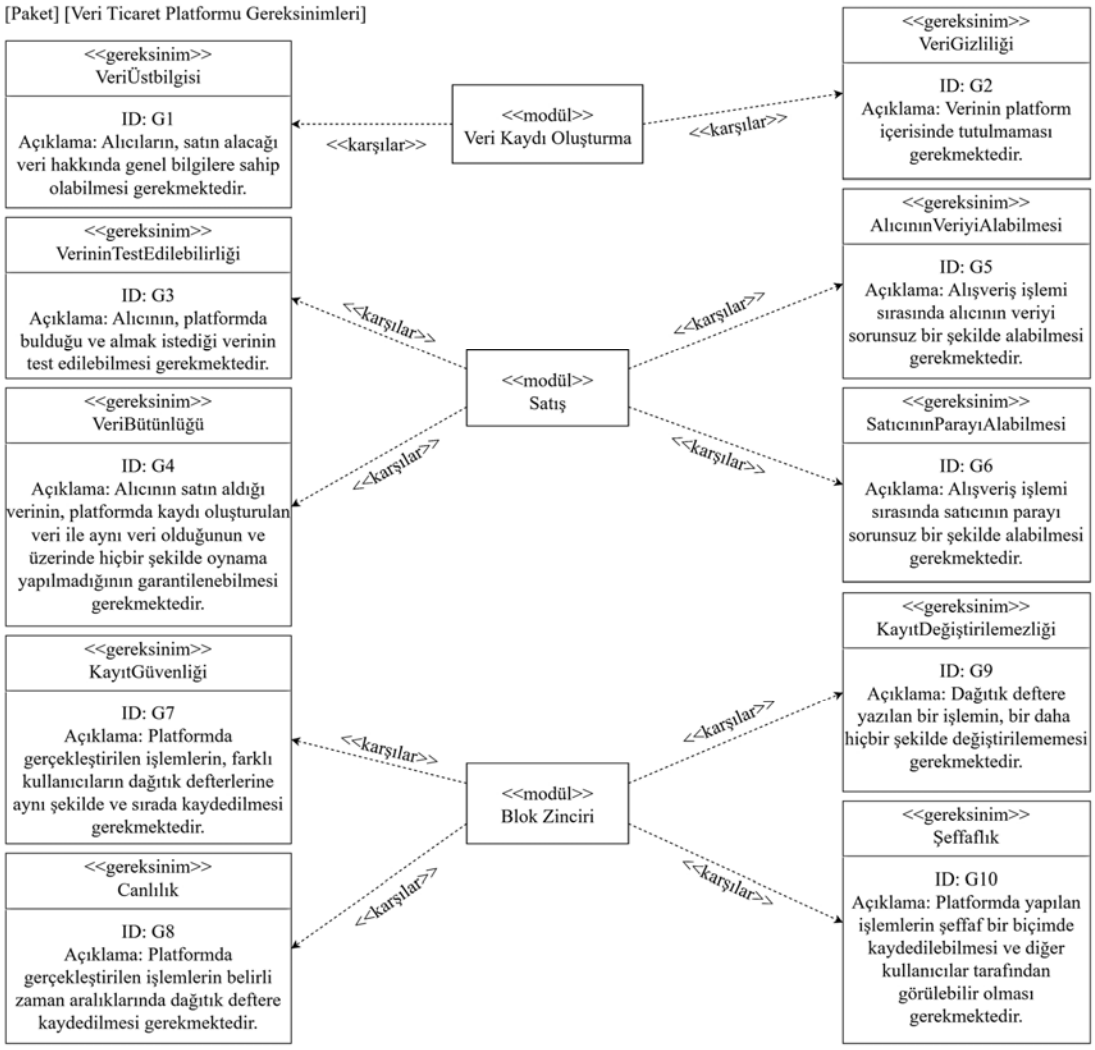
Dağıtık kayıt defteri, belirli bir ağ veya ağ grubu üzerinde dağıtılmış olan ortak bir veri tabanı sistemidir. Ağdaki her kullanıcı bu defterin lokal bir kopyasına sahip olabilir ve defter üzerinde yapılan değişiklikler uzlaşı protokolleri vasıtasıyla belirli aralıklarla bu kopyaların tamamına yansıtılmaktadır. Sağlam bir dağıtık kayıt



Şekil 3. "Satış" modülü ("Trading" module)



Şekil 4. "Blok işleme" modülü ("Block processing" module)



Şekil 5. Gereksinim diyagramı (Requirement diagram)

defterinin güvenlik ve canlılık olmak üzere iki temel gereksinimi karşılaması beklenir. İlk gereksinim, deftere yazılacak işlemlerin ağdaki kullanıcılar tarafından ortak bir mutabakata varılarak yazılacağını belirtirken; ikincisi, doğru bir şekilde gerçekleştirilmiş bir işlemin ağdaki kullanıcılar tarafından er ya da geç onaylanarak deftere yazılacağını belirtmektedir. Bu çalışmada dağıtık kayıt defteri sisteminin blok zinciri teknolojisi üzerinden gerçekleştirildiği varsayılmaktadır.

Kötü niyetli bir kullanıcı kendi adına menfaat sağlamak için, dağıtık defter içerisinde yapılmış bir ticaretin kayıtları üzerinde oynayarak o ticaret hiç yapılmamış gibi gösterebilir. Benzer şekilde hiç yapılmamış bir ticaretin de, dağıtık defterdeki kayıtlar üzerinde oynanarak yapılmış gibi gösterilmesi mümkündür. Bu tür senaryolara karşı sistemi daha dirençli kılmak için dağıtık deftere yazılan bir işlemin, değiştirilemez bir şekilde saklanması gerekmektedir. Bu sayede kötü niyetli kullanıcıların sistemdeki kayıtları değiştirerek kendilerine menfaat sağlamasının önüne geçilecektir. Benzer şekilde kötü niyetli bir kullanıcı, otoritelerle anlaşarak işlemlerin eksik kaydedilmesini sağlayabilir ve bunun sonucunda alıcı veya satıcının itibarının zedelenmesine sebep olabilir. Bu sebeple platformda gerçekleştirilen işlemlerin şeffaf bir biçimde kaydedilebilmesi gerekmektedir. Bu sayede kaydedilen işlemler diğer kullanıcılar tarafından incelenebilir olacak ve platforma duyulan güven artacaktır.

2.6. Örnek Senaryo (Example Scenario)

Bu bölümde yukarıda bahsedilen gereksinimlerin nasıl karşılanabileceği örnek bir senaryo üzerinden tartışılacaktır.

Sistemde satış yapmak isteyen satıcı; sistem içerisinde alıcıların verileri daha rahat araştırabilmesine ve değerlendirebilmesine imkân sağlamak için verilere ait bir üst bilgi hazırlar ve bu üst bilgi üzerinden verilere ait bir kayıt oluşturur. Gereksinimler kısmında da bahsedildiği gibi, blok zinciri şeffaf bir sistem olduğu için verilerin gizliliğini sağlamak adına satıcı verileri lokal depolama alanında saklayabileceği gibi şifreli olarak bir bulut depolama sisteminde de tutabilir.

Alıcılar platform üzerinde oluşturulan verilere ait kayıtları blok zinciri vasıtasıyla görüntüleyebilmektedir. Alıcılar bu verilerden birini satın almak istediğinde satış modülü üzerinden ilgili satıcıyla irtibata geçerler. Alışveriş işleminden önce sistemin alıcıya veriyi test edebilme imkânı vermesi gerekmektedir. Verinin test edilebilirliği diye adlandırdığımız bu gereksinim satıcının veriye ait küçük bir parçayı alıcıyla paylaşması yoluyla sağlanabilir. Bu noktada paylaşılan bu parçanın veriye ait olduğunun kanıtlanması gerekmektedir. Bununla birlikte satıcının verinin başlangıçta kaydı oluşturulan veri ile aynı olduğunu ve değiştirilmediğini, diğer bir

ifadeyle verinin bütünlüğünün sağlandığını da alıcıya ispat etmesi gerekmektedir. Bu iki gereksinim sisteme entegre edilecek *Alan Kanıtı* modülü vasıtasıyla sağlanabilir.

Bunların yanı sıra yukarıda da belirtildiği gibi *Satış* modülü ile ilintili karşılanması gereken alıcının veriyi ve satıcının parayı alabilmesi olarak adlandırdığımız gereksinimler sisteme entegre edilebilecek *Akıllı Sözleşme* modülü üzerinden karşılanabilirler. Alan kanıtı protokolünün uygulanmasına imkân sağlayacak *Alan Kanıtı* modülünün ve akıllı sözleşme çalıştırmamıza imkân sağlayacak *Akıllı Sözleşme* modülünün nasıl çalıştıklarına geçmeden önce Alan kanıtı protokolünü ve akıllı sözleşme kavramını kısaca açıklamak yerinde olacaktır.

2.7. Alan Kanıtı (Proof of Space)

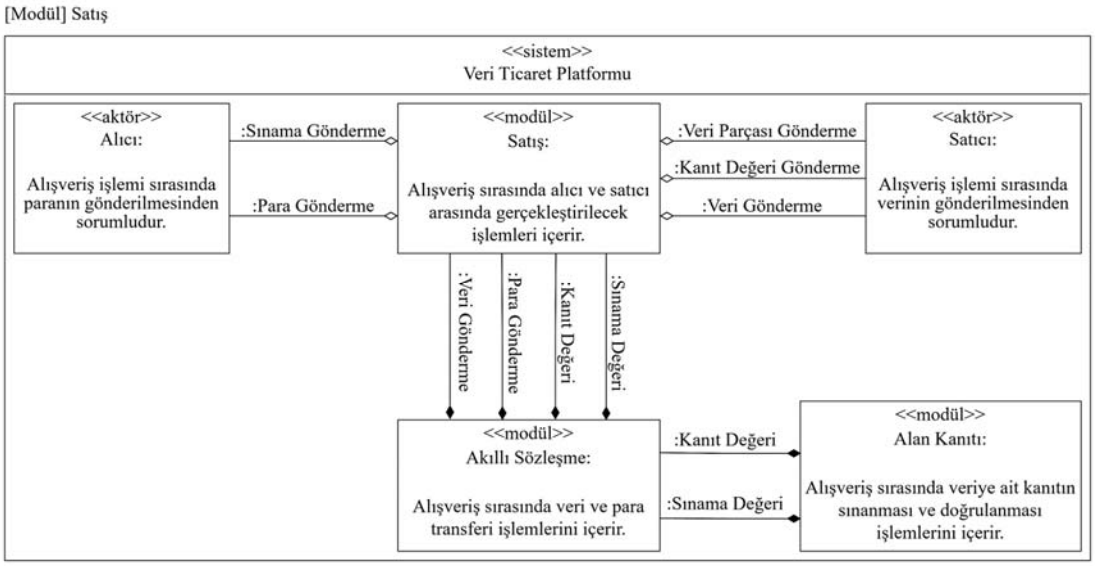
Kullanılan cihazdaki bellek alanına dayanan, ispatlayıcı ve onaylayıcı olarak adlandırılan iki kullanıcı arasında gerçekleştirilen bir protokoldür. Protokol, ispatlayıcıya lokal belleğinde spesifik bir amaç için tahsis ettiği alanın belirlenen süre içerisinde sadece o amaç doğrultusunda değiştirilmeden korunduğunu ispat etme imkânı vermektedir. Protokol iki aşamadan oluşmaktadır. İlk aşamada ispatlayıcı N-bitlik bir veriyi lokal belleğine kaydeder ve ikinci aşamada kullanılmak üzere bu verinin bir özeti sayılabilecek veriyi lokal belleğinde sakladığına dair bir taahhüt değerini üretip onaylayıcıyla paylaşır. İkinci aşamada onaylayıcı ispatlayıcının ilgili veriyi orijinal haliyle tutup tutmadığını test etmek için rastgele bir sınama değeri oluşturur ve bu değeri ispatlayıcıyla paylaşır. Bu aşamada ispatlayıcı sınama değerine karşılık gelen ve veriyi orijinal haliyle sakladığını ispat eden bir kanıt değeri oluşturur ve bu kanıt değerini onaylayıcıyla paylaşır. Son olarak onaylayıcı ispatlayıcının ilk aşamada paylaştığı taahhüt değeriyle uyumlu bir kanıt değeri oluşturulup oluşturulmadığını kontrol ederek kanıt değerini kabul eder ya da reddeder. İspatlayıcı ve onaylayıcı arasında karşılıklı etkileşim gerektiren alan kanıtı yöntemi ilk olarak Dziembowski vd. [20] tarafından önerilmiş bir uzlaşı algoritması olup, önerilen yöntemde kanıt oluşturma işlemlerinde Merkle ağaç yapısı kullanılmış ve bu sayede ikinci aşamada üretilen kanıt değerinin orijinal dosyaya göre oldukça düşük boyutta üretilmesi sağlanmıştır.

Sınama değerinin alıcı tarafından belirlenmesi ve sınama miktarına bir sınır konulmaması, kötü niyetli bir alıcının birden fazla farklı sınama değeri göndererek verinin bir kısmına ya da tamamına ulaşabilmesine neden olabilir. Bu durumu engellemek için alıcının dosyanın hangi parçasını kontrol edeceğini belirleyen sınama değerinin rastgele belirlenmesi ve bu rastgeleliğin, alıcının manipüle edemeyeceği platformdaki herkesin katkı sağladığı blok zincirinden üretilmesi yerinde olacaktır. Bu noktada örneğin sınama için satıcıya gönderilecek değer, blok zincirindeki son bloğun özet değerinden üretilebilir.

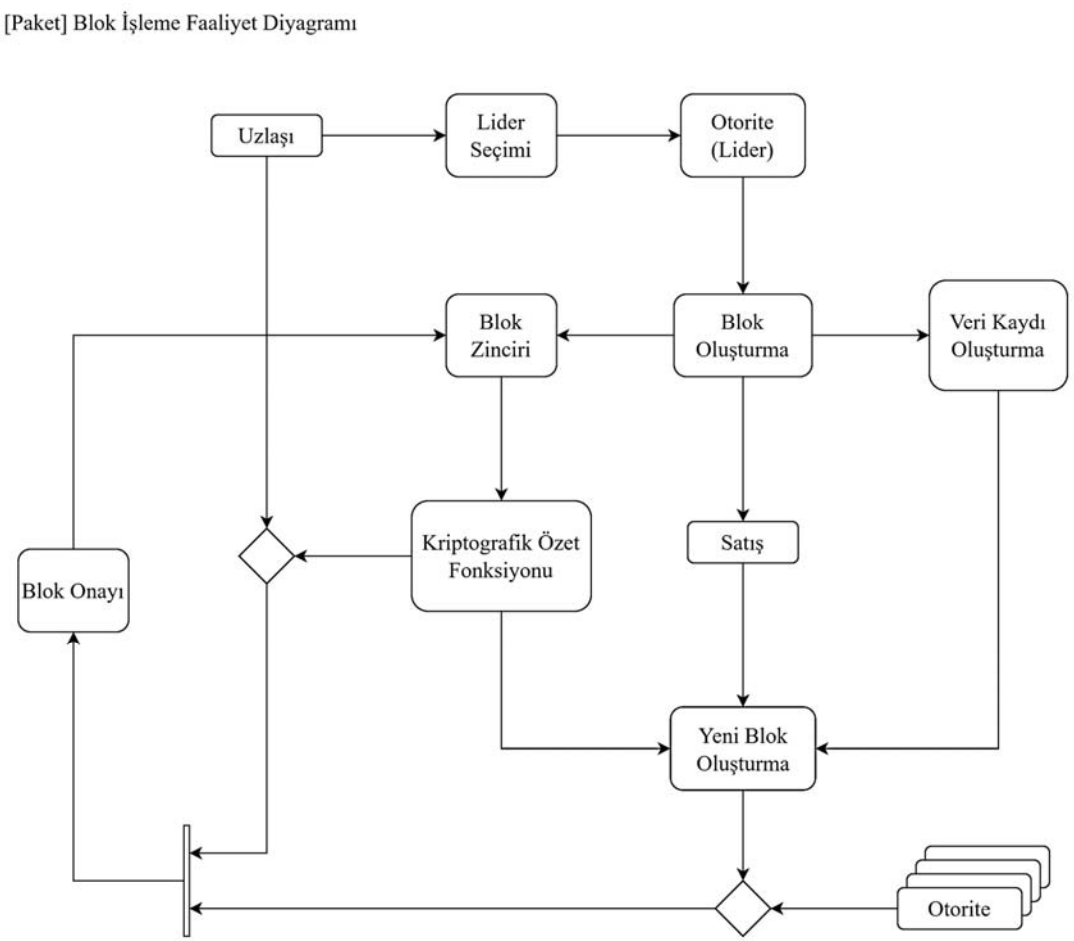
2.8. Akıllı Sözleşme (Smart Contract)

Blok zinciri üzerinde çalışan; içerisinde belirli sayıda kurallar ve yapılacak işlemler barındırarak, yalnızca bu kurallar sağlandığında işleyen bir bilgisayar kodudur. Bir akıllı sözleşme, çalışmaya başladıktan sonra hiçbir şekilde değiştirilemez veya durdurulamaz. Çoğunlukla para veya veri gibi değerli varlıkların takasında kullanılır ve üçüncü partileri ortadan kaldırdığı için işlem masraflarını düşürür. Ayrıca bir akıllı sözleşmenin çıktısı, sistemdeki diğer kullanıcılar tarafından kolaylıkla kontrol edilebilir ve onaylanabilir olduğu için güvenilirdir.

Yukarıda da ifade edildiği gibi bir önceki bölümde belirlenen ve Şekil 6'da gösterilen *Satış* modülü ile ilgili gereksinimler sisteme entegre edilen *Alan Kanıtı* ve *Akıllı Sözleşme* modülleri yardımıyla karşılanabilirler. *Alan Kanıtı* modülünde Dziembowski vd. [20] tarafından önerilmiş Merkle ağaç yapısı uygulanarak gerçekleştirilen alan kanıtı protokolü kullanılacaktır. Alan kanıtı protokolünün sağlıklı bir şekilde çalışabilmesi için satıcıların satmak istedikleri verilerle ilgili kayıt oluştururken alan kanıtında kullanılmak üzere verilere ait taahhüt değerini de veri üst bilgisine eklemeleri gerekmektedir. Bu noktada satıcılar ellerindeki veriyi önce n parçaya bölerler ve bu parçalar üzerinden bir Merkle ağacı oluştururlar. Sonrasında ilgili Merkle ağacının kökünü ve n sayısını taahhüt değeri olarak veri üst bilgisine eklerler. Alıcı platformdaki verilerden birini almak istediğinde; önce veriyi test edebilmek ve aynı zamanda veri bütünlüğünün ispatı için uygulanacak alan kanıtı protokolünde kullanılmak üzere, $\{1, \dots, n\}$ kümesinden bir sayıyı rastgele bir şekilde sınama değeri olarak belirleyip satış modülü üzerinden ilgili satıcıya ve *Akıllı Sözleşme* modülüne gönderir. Sonrasında satıcı *Satış* modülü üzerinden sınama değerine karşılık gelen veri parçasını alıcıya ve veri parçasıyla beraber alan kanıtı protokolünde kullanılmak üzere oluşturduğu kanıt değerini *Akıllı Sözleşme* modülüne gönderir. Veri



Şekil 6. Örnek senaryo için "Satış" modülü ("Trading" module for example scenario)



Şekil 7. Blok işleme faaliyet diyagramı (Activity diagram for block processing)

parçasını değerlendiren alıcı eğer veriyi almak isterse *Satış* modülü üzerinden *Akıllı Sözleşme* modülüne satış işlemi için gerekli olan parayı ve satıcıya bu isteğini gönderir. Satıcı bu isteğin karşılığı olarak veriyi *Akıllı Sözleşme* modülüne gönderir. Blok zinciri şeffaf bir sistem olduğundan platform içerisinde verinin direk paylaşılması veri gizliliği gereksinimi ile çelişeceğinden dolayı, satıcının veriyi ya da veri eğer bulut depolamada tutuluyorsa ilgili gizli anahtarı alıcının kimliğiyle şifreleyip ilgili şifreyi *Akıllı Sözleşme* modülüne göndermesi daha sağlıklı olacaktır. Diğer yandan, *Akıllı Sözleşme* modülü veri bütünlüğünün sağlanıp sağlanmadığını kontrol etmek için; *Alan Kanıtı* modülü üzerinden alıcıdan gelen sınama değeri, satıcıdan gelen kanıt değeri ve öncesinde zincire eklenmiş ilgili taahhüt değeri üzerinde alan kanıtı protokolünü çalıştırır. Eğer alan kanıtı protokolü verinin bütünlüğünü doğrularsa *Akıllı Sözleşme* modülü veri – para takasını gerçekleştirecektir.

Platformda gerçekleştirilen işlemler periyodik olarak uzlaşı modülü üzerinden belirlenen lider tarafından bloklara yazılmakta ve yine uzlaşı modülü üzerinden çalıştırılan uzlaşı protokolü üzerinden onaylanarak zincire eklenmektedir. Şekil 7'deki faaliyet diyagramında da görüleceği gibi önce uzlaşı modülü üzerinden yeni bloğu oluşturacak lider seçilir. Sonrasında lider seçilen otorite ilgili zaman aralığında platformda paylaşılan işlemler üzerinden yeni bir bloğa oluşturur. Liderler ayrıca sağlam bir zincir elde edebilmek amacıyla, çakışmaya dirençli kriptografik bir özet fonksiyonunu zincire son eklenmiş blok üzerinde çalıştırarak bir özet değeri oluştururlar ve bu değeri yeni bloğun başına yazarlar. Bu şekilde her bir bloğun çakışmaya dirençli kriptografik bir özet fonksiyonu üzerinden bir sonraki bloğa bağlanması sayesinde blokların kırılamaz bir zinciri elde edilmiş olmaktadır. Bu da bloklara işlenen kayıtların değiştirilemez bir biçimde saklanmasına imkân vermektedir.

Sonrasında liderler oluşturdukları blokları platformun diğer kullanıcılarıyla paylaşırlar. Platformun bu yapısı platformda gerçekleştirilen işlemlerin platforma kayıtlı bütün kullanıcılarca şeffaf bir biçimde görülebilmesine imkân tanıyacaktır. Yeni oluşturulan bloğu alan diğer otoriteler bloktaki işlemleri ve bloğun başına yazılan özet değerini doğruladıktan sonra ilgili bloğu zincire eklerler. Platformdaki diğer kullanıcıların bloğun doğruluğunu kontrol etme gibi bir sorumluluğu yoktur. Diğer kullanıcılar bu süreçten bağımsız olarak istediklerinde platformdaki otoritelerden biriyle irtibata geçerek ellerindeki zinciri güncellerler. İkinci bölümde de belirtildiği gibi platform izinsiz blok zinciri kullanılarak hayata geçirileceğinden, çok sayıda oyuncuyu tolere edebilen emeğin kanıtı [21] ya da hisse kanıtı [22] gibi algoritmalar çalıştıran çekiliş tabanlı uzlaşı protokolleri kullanmak platformun verimliliğini artıracaktır. Ayrıca Garay vd. [23] ve David vd. [22] yukarıda zikredilen sırasıyla emeğin kanıtı ve hisse kanıtı tabanlı uzlaşı protokollerinin canlılık ve güvenlik gereksinimlerini karşıladığını formel olarak göstermişlerdir.

3. Sonuçlar (Conclusions)

Bu çalışmada nesnelerin interneti yoluyla toplanan verilerin blok zinciri teknolojisi kullanılarak güvenilir ve sağlıklı bir şekilde

pazarlanabilmesi problemi ele alınmıştır. Bu noktada öncelikli olarak literatürdeki benzer çalışmalar incelenmiş ve ilgili çalışmaların eksiklikleri analiz edilmiştir. Bu analiz üzerinden SysML diyagramları yardımıyla blok zinciri tabanlı ideal bir veri ticaret platformunun nasıl olması gerektiği irdelenmiştir. Bu doğrultuda önce ilgili platformun bileşenleri belirlenmiş ve bu bileşenler arasındaki ilişkiler analiz edilmiştir. Ayrıca bahsi geçen sistemin güvenli ve etkili bir biçimde çalışabilmesi için ihtiyaç duyulan gereksinimler tanımlanmış; dahası, bu gereksinimlerin nasıl karşılanabileceği örnek bir senaryo üzerinden gösterilmiştir.

Kaynaklar (References)

1. Khan M.A., Salah K., IoT security: Review, blockchain solutions, and open challenges, Future Gener. Comput. Syst., 82, 395-411, 2018.
2. Galetsia P., Katsaliakia K., Kumar S., Big data analytics in health sector: Theoretical framework, techniques and prospects, Int. J. Inf. Manage., 50, 206-216, 2020.
3. Kamilaris A., Fonts A., Prenafeta-Boldú F.X., The rise of blockchain technology in agriculture and food supply chains, Trends Food Sci. Technol., 91, 640-652, 2019.
4. Yumna H., Khan M.M., Ikram M., Ilyas S., Use of Blockchain in Education: A Systematic Literature Review, Intelligent Information and Database Systems, Yogyakarta-Endonezya, 191-202, 8-11 Nisan, 2019.
5. McGhin T., Choo K.R., Liu C.Z., He D., Blockchain in healthcare applications: Research challenges and opportunities, Journal of Network and Computer Applications, 135, 62-75, 2019.
6. Kar A.K., Navin L., Diffusion of blockchain in insurance industry: An analysis through the review of academic and trade literature, Telematics and Informatics, 58, Makale No: 101532, 2021.
7. Tzianos P., Pipelidis G., Tsiamitros N., Hermes: An Open and Transparent Marketplace for IoT Sensor Data over Distributed Ledgers, IEEE International Conference on Blockchain and Cryptocurrency, Seul-Güney Kore, 167-170, 14-17 Mayıs, 2019.
8. Manzoor A., Liyanage M., Braeke A., Kanhere S.S., Ylianttila M., Blockchain based Proxy Re-Encryption Scheme for Secure IoT Data Sharing, IEEE International Conference on Blockchain and Cryptocurrency, Seul-Güney Kore, 99-103, 14-17 Mayıs, 2019.
9. Papadodimas G., Palaiokrasas G., Litke A., Varvarigou T., Implementation of smart contracts for blockchain based IoT applications, International Conference on the Network of the Future, Poznan-Polonya, 60-67, 19-21 Kasım, 2018.
10. An B., Xiao M., Liu A., Gao G., Zhao H., Truthful Crowdsensed Data Trading Based on Reverse Auction and Blockchain, Database Systems for Advanced Applications, Chiang Mai-Tayland, 292-309, 22-25 Nisan, 2019.
11. Chen C., Wu J., Lin H., Chen W., Zheng Z., A Secure and Efficient Blockchain-Based Data Trading Approach for Internet of Vehicles, IEEE Trans. Veh. Technol., 68 (9), 9110-9121, 2019.
12. Kiyomoto S., Fukushima K., Fair-trading protocol for anonymised datasets requirements and solution, International Conference on Information Management, Oxford-Birleşik Krallık, 13-16, 25-27 Mayıs, 2018.
13. Elbüz A., Osmanoğlu M., Tanrıöver Ö., Designing a Secure Blockchain-based Trading Platform for Internet of Things, Communications Faculty of Sciences University of Ankara Series A2-A3 Physical Sciences and Engineering, 61 (1), 102-110, 2019.
14. Dai W., Dai C., Choo K.R., Cui C., Zou D., Jin H., SDTE: A Secure Blockchain-Based Data Trading Ecosystem, IEEE Trans. Inf. Forensics Secur., 15, 725-737, 2019.
15. Guan Z., Shao X., Wan Z., Secure Fair and Efficient Data Trading Without Third Party Using Blockchain, International Conference on Internet of Things and Green Computing and Communications and Cyber, Physical and Social Computing and Smart Data, Halifax-Kanada, 1395-1401, 30 Temmuz-3 Ağustos, 2018.
16. Huang Z., Su X., Zhang Y., Shi C., Zhang H., Xie L., A decentralized solution for IoT data trusted exchange based-on blockchain, International Conference on Computer and Communications, Çengdu-Çin, 1180-1184, 13-16 Aralık, 2017.
17. Sabounchi M., Wei J., Roche' R., Blockchain-Enabled Peer-to-Peer Data Trading Mechanism, International Conference on Internet of Things and Green Computing and Communications and Cyber, Physical and Social Computing and Smart Data, Halifax-Kanada, 1410-1416, 30 Temmuz-3 Ağustos, 2018.
18. Wang Z., Tian Y., Zhu J., Data Sharing and Tracing Scheme Based on Blockchain, International Conference on Logistics, Informatics and Service Sciences, Toronto-Kanada, 1-6, 3-6 Ağustos, 2018.
19. Zheng S., Pan L., Hu D., Li M., Fan Y., A Blockchain-Based Trading Platform for Big Data, IEEE Conference on Computer Communications Workshops, Toronto-Kanada, 991-996, 6-9 Temmuz, 2020.
20. Dziembowski S., Faust S., Kolmogorov V., Pietrzak K., Proofs of Space, https://eprint.iacr.org/2013/796, 2013.
21. Nakamoto S. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf. Yayın tarihi 2008. Erişim tarihi Ekim 15, 2021.
22. David B., Gaži P., Kiayias A., Russell A., Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain, EUROCRYPT 2018, Tel Aviv-İsrail, 66-98, 29 Nisan-3 Mayıs, 2018.
23. Garay J., Kiayias A., Leonardos N., The Bitcoin Backbone Protocol: Analysis and Applications, EUROCRYPT 2015, Sofya-Bulgaristan, 281-310, 26-30 Nisan, 2015.